

EXTRACTING A UNIFORM RANDOM BIT-STRING OVER JACOBIAN OF HYPERELLIPTIC CURVES OF GENUS 2

BERNADETTE FAYE

ABSTRACT. Here, we proposed an improved version of the deterministic random extractors *SEJ* and *PEJ* proposed by R. R. Farashahi in [5] in 2009. By using the Mumford's representation of a reduced divisor D of the Jacobian $J(\mathbb{F}_q)$ of a hyperelliptic curve \mathcal{H} of genus 2 with odd characteristic, we extract a perfectly random bit string of the sum of abscissas of rational points on \mathcal{H} in the support of D . By this new approach, we reduce in an elementary way the upper bound of the statistical distance of the deterministic randomness extractors defined over \mathbb{F}_q where $q = p^n$, for some positive integer $n \geq 1$ and p an odd prime.

1. INTRODUCTION

The problem of converting random points of a variety (e.g a curve or Jacobian of a curve) into random bits has several cryptographic applications. Such applications are key derivation functions, key exchange protocols and design of cryptographically secure pseudorandom number generators. However the binary representation of the common secret element is *distinguishable* from a uniformly random bit-string of the same length. Hence one has to convert this group element into a random-looking bit-string. This can be done using a deterministic extractor.

Randomness extractors are having more and more applications in computer sciences, both in theory and in applications. Randomness extractors are objects that turn *weak* randomness into almost *ideal* randomness. For example, they can be used in designing key exchange protocols and are secure pseudorandom generators in the standard model.

Nowaday, it's a routine matter to extract randomness from a single source using arithmetic of finite fields or Elliptic curves. However, some subexponential attacks against the discrete logarithm problem on some elliptic curves are known. A recommendation is to move on Jacobian varieties (i.e hyperelliptic curves) of genus less or equals to 3. In 1989, Koblitz N. [9] proposed a cryptosystem based on hyperelliptic curves. Since then, hyperelliptic curves have gained a lot of interest for cryptographic applications. Furthermore, they were shown to be competitive with elliptic curves in speed and security. In [8], the security of genus 2 hyperelliptic curves is assumed to be similar to that of elliptic curves of the same group size.

At this moment, several deterministic extractors for elliptic curves are known. We refer to [3],[2],[6],[7] and the references therein. In our knowledge, few works have been done on randomness extractors of Jacobian of hyperelliptic curves. In general terms the problem can be described as follows. Given an algebraic variety \mathcal{V} over \mathbb{F}_q and one or

several sources of random but not necessarily uniformly generated points on \mathcal{V} , design an algorithm to generate long strings of random bits with a distribution that is close to uniform. In [4], Dvir has considered the problem of constructing randomness extractors for algebraic varieties. His construction requires only one but rather uniform source of points on \mathcal{V} . In fact, the task of extraction from an algebraic variety generalize the problem of extraction from affine sources which has drawn a considerable attention for cryptographic applications.

In this paper, we proposed an improved version of the extractors *SEJ* and *PEJ* from [5] for $J(\mathbb{F}_q)$, where $q = p^n$ for some positive integer n , the Jacobian of a genus 2 hyperelliptic curve \mathcal{H} defined over \mathbb{F}_q . In fact, for a given reduced divisor D of $J(\mathbb{F}_q)$ we used the Mumford's representation of D and extract a perfectly random bit string of the coordinate of its undeterminate corresponding to the sums of the abscissas of the rational points on \mathcal{H} in the support of D . The element extracted from D chosen randomly in $J(\mathbb{F}_q)$ is statistically close to uniform in \mathbb{F}_q . Instead of computing directly the statistical distance between the value of the element extracted from D and a random variable in \mathbb{F}_q as done by Farashahi in [5], we compute first the collision probability by summing over polynomials of degree less or equal to 2 in $\mathbb{K}[X]$, where \mathbb{K} is any subfield of $\overline{\mathbb{F}_q}$.

The remainder of this paper is organized as follows. In Section 2, we recall some definitions and results on the measurement parameters of randomness and bounds on character sums with polynomial arguments. In sections 3.1 and 3.2, we present and analyze the security of the modified version of the randomness extractors defined over \mathbb{F}_{p^n} and \mathbb{F}_p , respectively. We show that the outputs of these extractors, for a given uniformly random point of \mathbb{F}_q , are statistically close to a uniformly random variable in \mathbb{F}_q . For the analysis of these extractors, we need some bounds on the cardinalities of the character sums over polynomial defined over $\mathbb{K}[X]$. We give our estimates for them using Mordell's bound for polynomial of degree ≤ 2 .

2. PRELIMINARY RESULTS

In this section, we recall basics definitions and notations that will be used throughout the paper.

Notation. : For a finite field \mathbb{F} , we note by $\overline{\mathbb{F}}$ the algebraic closure of the field \mathbb{F} . Along this paper, \mathbb{F}_q is a finite field with q elements where $q = p^n$, with p an odd prime and $n \in \mathbb{N}^*$. Let E be a curve defined over \mathbb{F}_q , then the set of \mathbb{F}_q -rational points on E is denoted by $E(\mathbb{F}_q)$. Let \mathbb{K} be any subfield of $\overline{\mathbb{F}_q}$ and \mathcal{H} be an imaginary hyperelliptic curve, then we denote by $J_{\mathcal{H}}(\mathbb{K})$, the Jacobian of \mathcal{H} over \mathbb{K} . We denote by $\mathbb{K}[X]_{\leq d}$ the sets of polynomial in $\mathbb{K}[X]$ of degree less or equal to d . Further, let $lsb_k(x)$ be the k -least significant bits of a random element in \mathbb{F}_q .

2.1. Hyperelliptic Curves.

Definition 1. Jacobian of Hyperelliptic Curves

Let \mathcal{H} be an Hyperelliptic curve of g in \mathbb{F}_q , where q is odd. Here, we consider \mathcal{H} to be an imaginary hyperelliptic curve. Then \mathcal{H} has a plane model of the form $y^2 = f(x)$, where f is a square-free polynomial and $\deg(f) = 2g + 1$. For any subfield \mathbb{K} of $\overline{\mathbb{F}_q}$ containing \mathbb{F}_q , the set

$$\mathcal{H}(\mathbb{K}) = \{(x, y) : x, y \in \mathbb{K}, y^2 = f(x)\} \cup \{P_\infty\},$$

is called the set of \mathbb{K} -rational points on \mathcal{H} . The point P_∞ is called the point at infinity for \mathcal{H} . A point P on \mathcal{H} , also written $P \in \mathcal{H}$, is a point $P \in \mathcal{H}(\mathbb{F}_q)$. The negative of a point $P = (x, y)$ on \mathcal{H} is defined as $-P = (x, -y)$ and $-P_\infty = P_\infty$.

Definition 2. Reduced divisors

For each nontrivial class of divisors in $J_{\mathcal{H}}(\mathbb{K})$, there exist a unique divisor D on \mathcal{H} over \mathbb{K} of the form

$$D = \sum_{i=1}^g P_i - rP_\infty$$

where $P_i = (x_i, y_i) \neq P_\infty$, $P_i \neq -P_j$, for $i \neq j$, and $r \leq g$. Such a divisor is called a reduced divisor on \mathcal{H} over \mathbb{K} . By using Mumford's representation [10], each reduced divisor D on \mathcal{H} over \mathbb{K} can be uniquely represented by a pair of polynomials $[u(x), v(x)]$, $u, v \in \mathbb{K}[x]$, where u is monic, $\deg(v) < \deg(u) \leq g$, and $u \mid (v^2 - f)$. Precisely $u(x) = \prod_{i=1}^r (x - x_i)$ and $v(x_i) = y_i$. The neutral element of $J_{\mathcal{H}}(\mathbb{K})$, denoted by \mathcal{O} , is represented by $[1, 0]$. Cantors algorithm, [1], efficiently computes the sum of two reduced divisors in $J_{\mathcal{H}}(\mathbb{K})$ and expresses it in reduced form.

2.2. Measure of Randomness.

Definition 3. Collision Probability

Let \mathcal{X} be a finite set and X an \mathcal{X} -valued random variable. The collision probability of X denoted by $\text{Col}(X)$, is the probability $\text{Col}(X) = \Pr[X = X'] = \sum_{x \in \mathcal{X}} \Pr[X = x]^2$.

Definition 4. Statistical Distance

Let \mathcal{X} be a finite set and X . If X and Y are \mathcal{X} -valued random variables. Then the statistical Distance between X and Y is define as

$$SD(X, Y) = \frac{1}{2} \sum_{x \in \mathcal{X}} |\Pr[X = x] - \Pr[Y = x]|.$$

Let $U_{\mathcal{X}}$ be a random variable uniformly distributed on \mathcal{X} and $\delta \leq 1$ be a positive real number. Then a random variable X on \mathcal{X} is said to be δ -uniform if $SD(X, U_{\mathcal{X}}) \leq \delta$.

Lemma 5. Relation between SD and $\text{Col}(X)$

Let X be a random variable over a finite set \mathcal{X} of size $|\mathcal{X}|$ and $\Delta = SD(X, U_{\mathcal{X}})$ the statistical distance between X and $U_{\mathcal{X}}$, $U_{\mathcal{X}}$ is be a random variable uniformly distributed on \mathcal{X} . Then

$$\text{Col}(X) \geq \frac{1 + 4\Delta}{|\mathcal{X}|}. \quad (1)$$

Definition 6. *Deterministic (\mathcal{Y}, δ) -extractor.*

Let \mathcal{X} and \mathcal{Y} be two sets. Let Ext be a function $\text{Ext} : \mathcal{X} \leftarrow \mathcal{Y}$. We say that Ext is a deterministic (\mathcal{Y}, δ) -extractor of \mathcal{X} if $\text{Ext}(U_{\mathcal{Y}})$ is δ -uniform on (\mathcal{Y}) . That is,

$$SD(\text{Ext}(U_{\mathcal{X}}), U_{\mathcal{X}}) \leq \delta.$$

2.3. Character Sums with Polynomial arguments.

Definition 7. *Character*

Let G be an abelian group. A character of G is a homomorphism from $G \rightarrow \mathbb{C}^*$. A character is trivial if it is identically 1. We denote the trivial character by ψ_0 .

Definition 8. Let \mathbb{F}_q be a given finite field. An additive character $\psi : \mathbb{F}_q^+ \rightarrow \mathbb{C}$ is a character ψ with \mathbb{F}_q considered as an additive group. A multiplicative character $\psi : \mathbb{F}_q^* \rightarrow \mathbb{C}$ is a character with $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ considered as a multiplicative group. We extend ψ to \mathbb{F}_q by defining $\psi(0) = 1$ if ψ is trivial, and $\psi(0) = 0$ otherwise. Note that the extended ψ still preserves multiplication.

The main interests of exponential sums is that they allow to construct some characteristic functions and in some cases we know good bounds for them. The use of these characteristic functions can permit to evaluate the size of these sets. We focus on certain character sums, those involving the character e_p defined as follows.

Theorem 9. *Multiplicative Characters of \mathbb{F}_p*

The multiplicative characters of \mathbb{F}_p , where p is a prime, are given by: $\forall x \in \mathbb{F}_p, e_p(x) = e^{\frac{2i\pi x}{p}} \in \mathbb{C}^*$.

Theorem 10. *Additive Characters of \mathbb{F}_q*

Suppose that $q = p^n$, where p is a prime and $n \geq 1$. The additive characters of \mathbb{F}_q are given by: $\psi(x) = e_p(\text{Tr}(x))$ where $\text{Tr}(x) = x + x^p + \dots + x^{p^{n-1}}$ is the trace of x .

Lemma 11. Let p be a prime number and G a multiplicative subgroup of \mathbb{F}_p^* .

- (1) If $a = 0$, $\sum_{x=0}^{p-1} e_p(ax) = p$.
- (2) For all $a \in \mathbb{F}_p^*$, $\sum_{x=0}^{p-1} e_p(ax) = 0$.

Proof. See [13] pp 69. □

Theorem 12. *Winterhof Bound*

Let V be an additive subgroup of \mathbb{F}_{p^n} and ψ an additive character of \mathbb{F}_{p^n} . Then

$$\sum_{a \in \mathbb{F}_{p^n}} \left| \sum_{x \in V} \psi(ax) \right| \leq p^n.$$

Proof. See [12] □

2.4. Elementary Bounds on character sums with polynomial arguments. .

Here we use the same presentation as in [11]. Let $P(X) \in \mathbb{F}_q[X]$ be a polynomial of degree at most d . It seems reasonable to expect the distribution of values of $P(x)$ as x varies in \mathbb{F}_q to be spread out of \mathbb{F}_q . In fact these values belong to a set V with probability about $|V|/q$.

One important way of measuring the uniformity of distribution is through the character sums:

$$\left| \sum_{x \in \mathbb{F}_q} \psi(P(x)) \right|.$$

There are several Theorems showing that this sum is small. In our case, we will use Mordell's bound which work for arbitrary polynomial with degree $\leq d$.

Theorem 13. (*Mordell's Bound*)

Let ψ be a non trivial additive character of \mathbb{F}_q and let $P(X)$ be a nonzero polynomial of degree $d < \text{char}(\mathbb{F}_q)$. Then

$$\left| \sum_{x \in \mathbb{F}_q} \psi(P(x)) \right| \leq O\left(d \cdot q^{1-\frac{1}{2d}}\right). \quad (2)$$

3. EXTRACTORS OVER JACOBIAN OF HYPERELLIPTIC

In this section, we propose an improved version of the extractors proposed by Farashahi in [5] on Jacobian of hyperelliptic curve of genus 2 with odd characteristic. In our case, instead of working directly with points on the Jacobian $J(\mathbb{F}_q)$, we use there Mumford's representation. Therefore, our source become a subset of the polynomial ring $\mathbb{F}_q[X]$ where $q = p^n$, with p an odd prime and $n \geq 1$. Our approach uses character sums with polynomial arguments.

Let $J(\mathbb{F}_q)$ be the Jacobian of the hyperelliptic curve \mathcal{H} . We recall that each reduced divisor D on \mathcal{H} over \mathbb{F}_q can be uniquely represented by a pair of polynomials $[u(x), v(x)]$, $u, v \in \mathbb{F}_q[x]$. D can also be uniquely represent by at most 2 points on \mathcal{H} . Then, there is a map

$$\begin{aligned} h : J(\mathbb{F}_q) &\longrightarrow \mathbb{F}_q[x]^2 \\ P + Q - 2P_\infty &\longmapsto [x^2 + u_1x + u_0, v_1x + v_0], \\ P - P_\infty &\longmapsto [x + u_0, v_0], \\ \mathcal{O} &\longmapsto [1, 0]. \end{aligned}$$

Therefore, we define the *Sum* and *Prod* extractors as the restriction of *SEJ* and *PEJ* to the first component of the image of h .

3.1. Sum and Product Extractors for Jacobian over \mathbb{F}_{p^n} .

We consider the function f_k defined as follow:

$$\begin{aligned} f_k : \mathbb{F}_q &\longrightarrow \mathbb{F}_p^k \\ x &\longmapsto (x_1, x_2, \dots, x_k) \end{aligned}$$

where $x = (x_1, x_2, \dots, x_n)$ with $x_i \in \mathbb{F}_p$.

Definition 14. *Sum Extractor*

The Sum extractor for the Jacobian $J(\mathbb{F}_q)$ of \mathcal{H} over \mathbb{F}_q is defined as the function $Sum : \mathbb{F}_q[X]_{\leq 2} \rightarrow \mathbb{F}_p^k$ by

$$Sum(D) = \begin{cases} f_k(-u_1) & \text{if } D = [x^2 + u_1x + u_0, v_1x + v_0], \\ f_k(-u_0) & \text{if } D = [x^2 + u_0, v_0], \\ 0 & \text{if } D = [1, 0]. \end{cases}$$

Definition 15. *Product Extractor*

The product extractor $Prod$ for the Jacobian $J(\mathbb{F}_q)$ of \mathcal{H} over \mathbb{F}_q is defined as the function $Prod : \mathbb{F}_q[X]_{\leq 2} \rightarrow \mathbb{F}_p^k$ by

$$Prod(D) = \begin{cases} f_k(u_0) & \text{if } D = [x^2 + u_1x + u_0, v_1x + v_0], \\ f_k(-u_0) & \text{if } D = [x^2 + u_0, v_0], \\ 0 & \text{if } D = [1, 0]. \end{cases}$$

Let A and B be \mathbb{F}_q -valued random variables that are defined as

$$A := Sum(D), \quad B := Prod(D),$$

where $D \in J(\mathbb{F}_q)$. In the next Theorem, we show that provided the divisor D is chosen uniformly in $J(\mathbb{F}_q)$, the element extracted from the divisor D by Sum or $Prod$ is indistinguishable from a uniformly random bit-string \mathbb{F}_p^k , with $k < n$.

Theorem 16. *Let $U_{\mathbb{F}_q}$ be a random variable uniformly distributed in \mathbb{F}_q . Then*

$$\begin{aligned} (1) \quad \Delta(A, U_{\mathbb{F}_q}) &= O\left(\frac{\sqrt{p^k}}{2\sqrt{q}(q+1)}\right), \\ (2) \quad \Delta(B, U_{\mathbb{F}_q}) &= O\left(\frac{\sqrt{p^k}}{2\sqrt{q}(q+1)}\right). \end{aligned}$$

Proof. Let Ψ be the set of all additive characters over \mathbb{F}_q . We put $f := Sum$ and $G = \mathbb{F}_q[X]_{\leq 2}$. We consider the following sets.

$$M = \{x_{k+1}\alpha_{k+1} + x_{k+2}\alpha_{k+2} + \dots + x_n\alpha_n, x_i \in \mathbb{F}_p\} \subset \mathbb{F}_p^n.$$

$$\mathbb{A} = \{u_1(x), u_2(x) \in G^2, \exists m \in M : f(u_1(x)) - f(u_2(x)) = m\}.$$

M is an additive subgroup of \mathbb{F}_q of order k . Thus $|M| = p^k$ with $k \geq 1$. Using Lemma 11, we construct the following characteristic function for \mathbb{A}

$$\mathbf{1}_{\mathbb{A}} = \frac{1}{p^n} \sum_{\psi \in \Psi} \psi(f(u_1(x)) - f(u_2(x)) - m)$$

wich is equal to 1 if $f(u_1(x)) - f(u_2(x)) = m$ and 0 otherwise. Therefore, we have that

$$|\mathbb{A}| = \frac{1}{p^n} \sum_{u_1(x) \in G} \sum_{u_2(x) \in G} \sum_{m \in M} \sum_{\psi \in \Psi} \psi(f(u_1(x)) - f(u_2(x)) - m).$$

Then

$$Col(A) = \frac{1}{|G|^2} |\mathbb{A}|.$$

It's well known that the number of unitary polynomials of degree equal to d in a polynomial field $\mathbb{F}_q[X]$ is q^d . Thus we have that $|G| = q^2 + q$. Thus, $|G|^2 = q^4 + 2q^3 + q^2$. Then, we have that

$$\begin{aligned} Col(A) &= \frac{1}{|G|^2 p^n} \sum_{u_1(x) \in G} \sum_{u_2(x) \in G} \sum_{m \in M} \sum_{\psi \in \Psi} \psi(f(u_1(x)) - f(u_2(x)) - m) \\ &= \frac{1}{|G|^2 p^k} p^{n-k} |G|^2 + \frac{1}{|G|^2 p^n} \sum_{u_1(x) \in G} \sum_{u_2(x) \in G} \sum_{m \in M} \sum_{\psi \neq \psi_0} \psi(f(u_1(x)) - f(u_2(x)) - m) \\ &= \frac{1}{p^k} + \frac{1}{|G|^2 p^n} \sum_{u_1(x) \in G} \sum_{u_2(x) \in G} \sum_{m \in M} \sum_{\psi \neq \psi_0} \psi(f(u_1(x)) - f(u_2(x)) - m) \\ &= \frac{1}{p^k} + \frac{1}{|G|^2 p^n} \sum_{\psi \neq \psi_0} \left(\sum_{u_1(x) \in G} \psi(f(u_1(x))) \right) \left(\sum_{u_2(x) \in G} \psi(-f(u_2(x))) \right) \left(\sum_{m \in M} \psi(-m) \right) \\ &\leq \frac{1}{p^k} + \frac{K^2}{|G|^2 p^n} \sum_{\psi \neq \psi_0} \left(\sum_{m \in M} \psi(-m) \right) \end{aligned} \quad (3)$$

where $K = \max_{\psi} \left(\left| \sum_{u_1(x) \in G} \psi(f(u_1(x))) \right|, \left| \sum_{u_2(x) \in G} \psi(-f(u_2(x))) \right| \right)$.

One note that the sum

$$\left| \sum_{u_1(x) \in G} \psi(f(u_1(x))) \right| \simeq \left| \sum_{x \in \mathbb{F}_q} \psi(P(x)) \right|$$

for a fix polynomial $P(x) \in \mathbb{F}_q[x]$. In fact, if $u_1(x)$ is of degree 2, then $|f(u_1(x))|$ is approximatively equal to $|u_1'(0)|$ and if $u_1(x)$ is of degree 1 then $|f(u_1(x))| \simeq |u_1(0)|$. Thus, we can assume $P(x)$ to be of degree $d = 1$. Therefore, Theorem 13 gives that

$$K \leq c_q \sqrt{q} \quad (4)$$

where c_q is the constant involved in inequality 2. Therefore, combining inequality (4) and Theorem 12, inequality 5 becomes

$$Col(A) \leq \frac{1}{p^k} + \frac{c_q^2 q}{q^4 + 2q^3 + q^2} = \frac{q^4 + 2q^3 + q^2 + c_q^2 p^k q}{p^k (q^4 + 2q^3 + q^2)}.$$

From Lemma 11, we have that

$$\frac{1 + 4\Delta^2(A, U_{\mathbb{F}_q})}{p^k} \leq \text{Col}(A) \leq \frac{q^4 + 2q^3 + q^2 + c_q^2 p^k q}{p^k(q^4 + 2q^3 + q^2)}.$$

Therefore,

$\Delta(A, U_{\mathbb{F}_q}) \leq \frac{c_q}{2\sqrt{p^{n-k}(p^n+1)}} = \frac{c_q\sqrt{p^k}}{2\sqrt{q}(q+1)}$, thus $\Delta(A, U_{\mathbb{F}_q}) = O\left(\frac{\sqrt{p^k}}{2\sqrt{q}(q+1)}\right)$. This finishes the proof of (1).

The proof of (2) can be done in a similar way, thus we omit the details. \square

Corollary 17. *The functions Sum and Prod are deterministic $\left(\mathbb{F}_p^k, O\left(\frac{\sqrt{p^k}}{2\sqrt{q}(q+1)}\right)\right)$ -extractor for $J(\mathbb{F}_q)$.*

Proof. The result of Theorem 16 gives the proof of this corollary. \square

3.2. Sum and Product Extractors for Jacobian over \mathbb{F}_p . Here we defined the Sum and Prod extractors as before on \mathbb{F}_p where p is a prime number ≥ 3 . We recall that if I is an interval of integers, it's well known that

$$\sum_{x \in \mathbb{F}_p} \left| \sum_{\sigma \in I} e_p(x\sigma) \right| \leq p \log_2(p).$$

Definition 18. *We defined the extractors $S_k : \mathbb{F}_p[X]_{\leq 2} \rightarrow \{0, 1\}^k$ by*

$$S_k(D) = \begin{cases} \text{lsk}_k(-u_1) & \text{if } D = [x^2 + u_1x + u_0, v_1x + v_0], \\ \text{lsb}_k(-u_0) & \text{if } D = [x^2 + u_0, v_0], \\ 0 & \text{if } D = [1, 0]. \end{cases}$$

and $P_k : \mathbb{F}_p[X]_{\leq 2} \rightarrow \{0, 1\}^k$ by

$$P_k(D) = \begin{cases} \text{lsk}_k(u_0) & \text{if } D = [x^2 + u_1x + u_0, v_1x + v_0], \\ \text{lsb}_k(-u_0) & \text{if } D = [x^2 + u_0, v_0], \\ 0 & \text{if } D = [1, 0]. \end{cases}$$

The following Lemmas states that S_k and P_k are deterministic extractors for the Jacobian of the hyperelliptic curve.

Lemma 19. *Let $G := \mathbb{F}_p[X]_{\leq 2}$ and U_G a random variable uniformly distributed in G and k a positive integer. Then*

$$\Delta(A, U_k) \ll \sqrt{\frac{2^k}{p}} \left(1 + \frac{\sqrt{\log_2(p)}}{p+1} \right)$$

where U_k is the uniform distribution on $\{0, 1\}^k$.

Proof. Let $\delta = 2^k$, $\sigma_0 := msb_{n-k}(p-1)$ and $A = S_k(D)$. We consider the set

$$\mathbb{A} = \{u_1(x), u_2(x) \in G^2, \exists \sigma \leq \sigma_0, S_k(u_1(x)) - S_k(u_2(x)) - \delta\sigma \equiv 0 \pmod{p}\}. \text{ Then}$$

$$Col(A) = \frac{1}{|G|^2} |\mathbb{A}|.$$

$$\begin{aligned} Col(A) &= \frac{1}{|G|^2 p} \sum_{u_1(x) \in G} \sum_{u_2(x) \in G} \sum_{\sigma \leq \sigma_0} \sum_{\psi \in \Psi} \psi(S_k(u_1(x)) - S_k(u_2(x)) - \delta\sigma) \\ &= \frac{\sigma_0 + 1}{p} + \frac{1}{|G|^2 p} \sum_{u_1(x) \in G} \sum_{u_2(x) \in G} \sum_{\sigma \leq \sigma_0} \sum_{\psi \neq \psi_0} \psi(S_k(u_1(x)) - S_k(u_2(x)) - \delta\sigma) \\ &= \frac{\sigma_0 + 1}{p} + \frac{1}{|G|^2 p} \sum_{u_1(x) \in G} \sum_{u_2(x) \in G} \sum_{\sigma \leq \sigma_0} \sum_{\psi \neq \psi_0} \psi(S_k(u_1(x)) - S_k(u_2(x)) - \delta\sigma) \\ &= \frac{\sigma_0 + 1}{p} + \frac{1}{|G|^2 p} \sum_{\psi \neq \psi_0} \left(\sum_{u_1(x) \in G} \psi(S_k(u_1(x))) \right) \left(\sum_{u_2(x) \in G} \psi(-S_k(u_2(x))) \right) \left(\sum_{\sigma \leq \sigma_0} \psi(-\delta\sigma) \right) \\ &\leq \frac{\sigma_0 + 1}{p} + \frac{K^2}{|G|^2 p} \sum_{\psi \neq \psi_0} \left(\sum_{\sigma \leq \sigma_0} \psi(-\delta\sigma) \right) \end{aligned} \tag{5}$$

$$\leq \frac{\sigma_0 + 1}{p} + \frac{p \log_2(p)}{|G|^2} \tag{6}$$

where $K = \max_{\psi} \left(\left| \sum_{u_1(x) \in G} \psi(S_k(u_1(x))) \right|, \left| \sum_{u_2(x) \in G} \psi(-S_k(u_2(x))) \right| \right) \leq \sqrt{p}$.

Therefore,

$$\Delta(A, U_k) \ll \sqrt{\frac{2^k}{p}} \left(1 + \frac{\sqrt{\log_2(p)}}{p+1} \right).$$

□

Lemma 20. Let $G := \mathbb{F}_p[X]_{\leq 2}$ and U_G a random variable uniformly distributed in G and k a positive integer. Then

$$\Delta(A, U_k) \ll \sqrt{\frac{2^k}{p}} \left(1 + \frac{\sqrt{\log_2(p)}}{p+1} \right)$$

where U_k is the uniform distribution on $\{0, 1\}^k$.

Proof. The proof for the extractor P_k is similar to the proof of Lemma (19). □

4. COMPARISON

We mainly compare our result with the result of R. R. Farashahi (see [5].) In fact, Farashahi obtained a $O(\mathbb{F}_q, \frac{1}{\sqrt{q}})$ -deterministic extractor by computing directly the statistical distance. His method of proof was more complicated and involved bounds of cardinalities of some curves.

In our approach, instead of computing directly the statistical distance, we compute the collision probability then use the inequality (1) to obtain a sharper estimate of the statistical distance. One sees that the upper bounds obtained in Theorem 16 are smaller than the bounds on *SEJ* in Proposition 1 and *PEJ* in Corollary 2 in [5].

Moreover, the output of the extractor *SEJ* in [5] is a coefficient $-u_1 \in \mathbb{F}_{p^k}$ of a polynomial of degree 2. Or, an element in \mathbb{F}_{p^k} is not necessarily a uniform random-bit string. But, in our case, we extract the k least significant bits of the coefficient $-u_1$ using the function f_k as defined in section 3.1. So, our approach gives more advantages for further applications in cryptography.

Furthermore, we have defined the extractors *Sum* and *Prod* on \mathbb{F}_p , where p is an odd prime. Our results obtained in Lemma 19 and Lemma 20 are, in our knowledge, new results in this subject.

ACKNOWLEDGMENTS

This work was carried out by a financial support from the government of Canada's International Development Research Centre (IDRC) and within the framework of the AIMS research for Africa project. The author thanks Dr. Abdoul A. Ciss for useful comments and suggestions on an earlier draft of this paper.

REFERENCES

- [1] Cantor, D. "Computing in the Jacobian of a Hyperelliptic Curve" *Mathematics of Computation* **48(177)**, (1989) 95-101.
- [2] C. Chevalier, P.-A. Fouque, D. Pointcheval and S. Zimmer, Optimal randomness extraction from a Diffie-Hellman element, *Proc Eurocrypt 2009, Lect. Notes in Comp. Sci., Springer-Verlag, Berlin*, **5479** (2009), 572-589.
- [3] A. A. Ciss and D. Sow, Randomness extraction in elliptic curves and secret key derivation at the end of Diffie Hellman protocol, *Intern. J. Appl. Cryptography*, **2** (2012), 360-365.
- [4] Z. Dvir, "Extractors for varieties", *Comput. Complex.*, **21** (2012), 515- 572.
- [5] R. R. Farashahi (2007) "Extractors for Jacobian of Hyperelliptic curves of genus 2 in odd Characteristic. In *S.D Galbraith (ED) Proceeding of the 11-th IMA International conference on Cryptography and Coding, 18-20 December 2007, Cirencester, United Kingdom. (pp 313-335). (Lecture notes in computer Science; Vol 4887) Berlin, Germany: Springer*. DOI: 10.1007/978-3-540-77272-9-19.
- [6] R. R. Farashahi and I. E. Shparlinski, Pseudorandom bits from points on elliptic curves, *IEEE Trans. Inform. Theory* **58** (2012), 1242- 1247.
- [7] R. R. Farashahi, P.-A. Fouque, I. E. Shparlinski, M. Tibouchi and J. F. Voloch, Indifferentiable deterministic hashing to elliptic and hyperelliptic curves, *Math. Comp.*, **82** (2013), 491-512.

- [8] Gaudry, P. "An Algorithm for Solving the Discrete Log Problem on Hyperelliptic Curves". *In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, 1807*, Springer, Heidelberg (2000), 3419-3448.
- [9] Koblitz, N., "Hyperelliptic Cryptosystem.", *J. of Cryptology*, **1** (1989), 139-150.
- [10] Mumford, D. "Tata Lectures on Theta II" *In: Progress in Mathematics, 43* (1984).
- [11] Swastik K. "Elementary bounds on character sums with polynomial arguments", Topics in Finite Fields (Fall 2013), Rutgers University. Last Modified: Thursday, 10-th October, 2013.
- [12] A. Winterhof, Incomplete Additive Character Sums and Applications, *In Finite fields and applications*. Springer Berlin Heidelberg, (2001) p. 462-474.
- [13] S. Zimmer, Mécanismes cryptographiques pour la génération de clefs et l'authentification, (2008). Thèse de doctorat. école normale supérieure.

UNIVERSITÉ CHEIKH ANTA DIOP DE DAKAR
 DEPARTEMENT DE MATHÉMATIQUES ET D'INFORMATIQUE
 BP: 5005, DAKAR-FANN
 DAKAR, SENEGAL.

AFRICAN INSTITUTE FOR MATHEMATICAL SCIENCES(AIMS)
 KM 2 ROUTE DE JOAL
 BP 1418 , MBOUR, SENEGAL AND
 SCHOOL OF MATHEMATICS
 UNIVERSITY OF THE WITWATERSRAND
 PRIVATE BAG X3, WITS 2050, SOUTH AFRICA.

E-mail address: `bernadette@aims-senegal.org`